# NATIONAL INSTITUTE OF TECHNOLOGY PATNA

## Department of Computer Science and Engineering

## End Semester Exam 2022

## Subject: Blockchain Technology (CS6475)

**Full Marks: 70** **Duration: 3 Hours**

---

**Answer any 7 questions. Make assumption of missing data if any.**
**Please write precise and to the point answers, irrelevant and lengthy answers may attract penalty.**

1. a.) Write a smart contract code in solidity which stores the four details of customer :– "customer_name", "account_number", "address" and "salary" for 10 customers and display the details of customer using a function DISPLAY (). [5]
   b.) Explain SHA-512 in detail with diagram. [5]

2. a.) Write a solidity program to store the name, roll_number, marks of 10 students. Also create a function MAX() which will display the student's name who got maximum marks. [5]
   b.) In RSA cryptosystem a particular A uses two prime numbers p=13 and q= 17 to generate her public key and private keys. If public key of A is 35. What is the private key of A. [5]

3. a.) Write a solidity program for signature verification. Also explain the process/ steps involved in the signature verification. [5]
   b.) Assume that the total hash power of the network stays constant, what is the probability that a block will be found in next 5 minutes. Suppose Bob the merchant wants to have a policy that order will be ship within $x$ minutes after receipt of payment. What value of $x$ should Bob choose so that with 99% confidence 5 blocks will be found within $x$ minutes. [5]

4. a.) Suppose you are using RSA algorithm-based cryptosystem to securely share the number of marbles that you have currently with you, among your friends. The private key you are using is (3, 15). Your friends know the corresponding public key is (11, 15). One of your friend wants to share the exact amount of marbles that your friend can have so that he/she can secretly share to you? [5]
   b.) Write a solidity program to print the name, age, branch and college_name using public variables. [5]

5. a.) Write a solidity program for transferring, receiving and withdrawing ethers. [5]
   b.) Explain Merkle tree and Merkle root. How does it differ in Ethereum network. [5]

6. a.) Differentiate PoW and PoS consensus. Expain Byzantine general problem. [5]
   b.) Analyze 51 % attack in PoW, PoS and PBFT consensus algorithm. [5]

7. a.) Differentiate between proof-of-work and Ethash. [5]
   b.) Can you device a meet-in-middle attack for a triple DES. [5]

8. Write short notes on: [2 x 5]
   a.) Delegated Proof of Stake (DPoS)
   b.) MD5
   c.) Differentiate public, private, consortium and hybrid blockchain.
   d.) DES
   e.) DApp.